Activity File: Interview Question

Domain: Cloud Security

Cloud Access Control

One of my projects was to deploy a cloud network and control access to said network, which was necessary to regulate and monitor permissions and restrict unwanted traffic to the virtual networks (VNs) and between machines on the network. There are two firewalls/Network Security Groups (NSGs) before each of the two VNs. In the beginning, the NSG blocked all traffic to and from the networks. Afterward, inbound security rules were implemented. The only public IP address authorized to connect to the NSGs is an IPv4 from the workstation used for this project, with destination to port 80, protocol - allow any.

The first VN is called “RedTeamNet” and has a JumpBoxProvisioner and an Ansible container that allows access via SSH - port 22 - allow TCP - to the other three VMs in the network. The JumpBoxProvisioner allows for the admins to connect to a centralized place then access the VMs from there.

VM's have been configured with SSH key access only, which is the most secure way to configure remote access. Network redundancy is also in place. If one VM is down, then the other two will continue working. In terms of security, redundancy ensures the reliability and availability of the system.

The second VN is called “RedTeamNet2” and contains an ELK VM with an elk-docker. Inbound rules allow HTTP connection from the workstation IPv4 to ports 5601, 9200, and 5044. The JumpBox from RedTeamNet VN can also access the ELK VM via SSH.

ELK VM has two tools installed and configured - Filebeat and Metricbeat. Ansible playbooks were created to automatically install Filebeat and Metricbeat to Damn Vulnerable Web Applications (DVWA), allowing for easy scalability.

The JumpBox represents a single point for attacks, in order to gain access to the VNs. It also may become a bottleneck and present a problem with scalability. Since the number of users may increase with time. An alternative to a Jump Box will be to use Virtual Private Network (VPN) in front of the VNs. For this project, a VPN was not necessary given the scale of it with only a few VMs in its networks.

There are many benefits to VPN. It can be integrated into the firewalls, providing additional security. VPN must also be configured to allow only SSH or remote desktop connections through it, if not, there will be unsecured access to the networks, compromising security.